Представленные классификации свидетельствуют о существовании разнообразных подходов к понятию операционного риска, а значит, и к методике его расчета. В настоящий момент практически в каждом документе или учебном пособии приводится один из вариантов классификации рисков. В большинстве случаев выбранные критерии не позволяют охватить все множество рисков, однако ряд основных рисков в экономической литературе фигурирует. Исходя их этого, достаточно частыми являются попытки классифицировать подмножества рисков, входящих в эти общие понятия.

Риск, связанный с регулирующими органами наиболее актуален для банковских организаций, поэтому он чаще встречается в сферах, связанных с банковской деятельностью. Риск ликвидности некоторые авторы включают в понятие рыночных рисков [1].

Данные материалы свидетельствуют о множественности подходов к основной терминологии в изучаемой предметной области, а их анализ позволяет нам говорить о необходимости создания единого глоссария в области операционных банковских рисков.

Список литературы

1. *Романов С. В.* Классификация рисков: принципы и критерии. URL: http://www.aup.ru/articles/finance/4.htm.

2. Базельский комитет по банковскому надзору «Международная конвергенция измерения капитала и стандартов капитала: новые подходы» // ЦБ РФ. Перевод «Базель II». URL: http://www.cbr.ru/today/ms/bn/Basel.pdf, ст. 644)

3. Письмо Банка России от 23 июня 2004 г. № 70-Т «О типичных банковских рисках».

УДК 004.056.53

Р. Д. Меньщиков, Е. В. Чудинова, В. В. Москвин
Научный руководитель: ст. преп. В. В. Москвин
Курганский государственный университет, Курган

COOKIE: ПРИНЦИПЫ РАБОТЫ И БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ

Аннотация. В данной статье описаны принцип работы и безопасность использования cookie файлов. Также рассмотрены основные преимущества и недостатки использования cookie, приведены настройки cookie в популярных веб-браузерах.

Ключевые слова: cookie; аутентификация; HTTP; браузер; XSS; защита данных.

В настоящее время информационные технологии развиваются очень стремительно. Немалый вклад в их развитие внесла глобальная сеть Интернет. Для просмотра всевозможных веб-страниц люди используют специальное прикладное программное обеспечение — браузеры.

Одним из основных компонентов, участвующих в процессе взаимодействия браузера и веб-сайта, являются cookie файлы — файлы, которые хранятся на компьютере пользователя и содержат в себе различные данные о посещенных сайтах. Используются они для аутентификации пользователя на веб-сайтах, хранения персональных настроек пользователя, отслеживания на сайте действий пользователя, сбора статистики [1].

Наличие в cookie логинов и паролей пользователя делает их потенциальной целью злоумышленников.

Cookie являются неотъемлемой частью протокола HTTP, с помощью которого осуществляется взаимодействие между браузером и веб-страницами. Протокол HTTP стал набирать популярность с начала 90-х годов и в настоящее время на нем построена вся глобальная сеть Интернет. HTTP-протокол имеет клиент-серверную структуру передачи данных [2].

Алгоритм работы передачи cookie состоит из трех этапов: браузер → сервер, сервер → браузер, браузер → сервер. На первом этапе браузер выполняет HTTP-запрос для доступа к какой-либо веб-странице. На втором этапе сервер отправляет содержимое веб-страницы с указанием браузеру сохранить cookie. На третьем этапе браузер подтверждает получение cookie [3].

Механизм cookie используются уже более двух десятков лет. За это время они зарекомендовали себя в качестве эффективного средства, обладающего следующими преимуществами:

1. Сохранение персональных настроек пользователя для более эффективного серфинга по сети.
2. Простота реализации и использования.
3. Отсутствие повторного ввода данных аутентификации.

К тому же работа с большинством интернет-магазинов не представляется возможной без cookie-файлов.

Кроме того, cookie файлы обладают и рядом недостатков. Самыми значимыми являются низкий уровень безопасности, хранение cookie в простом текстовом формате, необходимость настройки веб-браузера.

Существует несколько вариантов атак на cookie. Один из них — кража cookie (XSS-атака). XSS-атака или межсайтовый скриптинг применяется для атаки на веб-сайты с целью похищения данных пользователей. Принцип действия атаки заключается в следующем:

1. Атакующий внедряет вредоносный код на веб-сайт.
2. Жертва посещает веб-сайт и активирует вредоносный код.

3. Вредоносный код похищает cookie жертвы и передает их на веб-сервер злоумышленника.

Еще один из видов атаки на cookie файлы — их подмена. Подмена cookie, в отличии от кражи, отличается тем, что при передаче cookie файлов на веб-сервер злоумышленник не перехватывает их, а вносит соответствующие изменения непосредственно в их содержимое.

Физический доступ к данным — вид атаки реализуем только при посредственном контакте с персональным компьютером жертвы. Принцип действия данной атаки состоит в следующем:

1. Злоумышленник копирует cookie файлы жертвы и переносит их на внешний накопитель.

2. Злоумышленник переходит на необходимый ресурс с украденными cookie.

3. Предоставляется полный доступ к данным жертвы.

Для защиты пользовательских данных в cookie от вышеперечисленных атак нужно придерживаться следующих рекомендаций:

1. Использовать защищенные соединения (SFTP, HTTPS).

2. Не переходить на сомнительные веб-ресурсы.

3. Не сохранять никакие персональные данные на веб-ресурсах при использовании публичных сетей Wi-Fi.

4. Своевременно удалять cookie и очищать кэш браузера.

5. Регулярно изменять пароли в аккаунтах.

6. Обновлять браузер и антивирусное ПО.

7. Настраивать использования cookie браузерами.

8. Использовать механизм приватных вкладок [4].

Есть также рекомендации для настроек хранения cookie:

1. Рекомендуется периодически анализировать хранящиеся на компьютере cookie на предмет наличия в них конфиденциальной информации. Создающие такие cookie сайты стоит внести в черные списки, разрешив для них только сеансовые cookie.

2. Запрещать прием сторонних cookie для сайтов, используемых исключительно для просмотра.

3. Рекомендуется хранить cookie для сайтов, имеющих сертификаты SSL с проверкой компании (Organization Validation), расширенной проверкой (Extended Validation).

Как показали исследования компании Positive Technologies, уязвимости, связанные с файлами cookie, стали наиболее часто встречающимися. Так, в 2016 году на первой строчке рейтинга наиболее популярных уязвимостей оказалась уязвимость среднего уровня риска «Межсайтовое выполнение сценариев» (Cross-Site Scripting), которая встречается в 75 % исследованных систем. А также уязвимости типа Insecure Session, которые позволяют злоумышленни-

ку перехватить значения cookie пользователя при реализации различных атак, оказались на пятом месте по распространенности (рис. 1) [5].

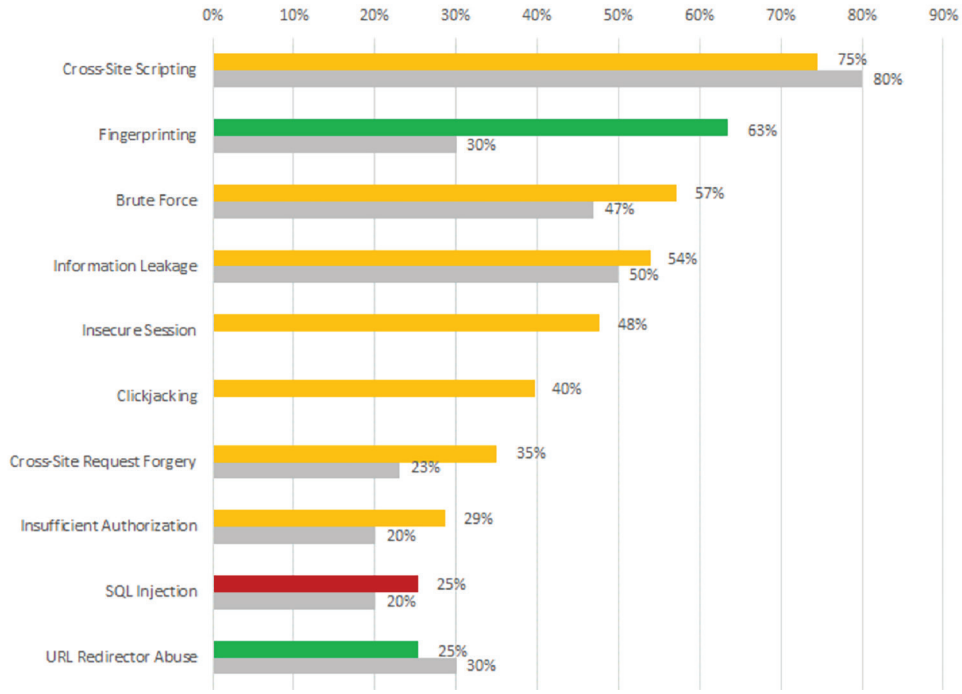

Рис. 1. Рейтинг наиболее популярных уязвимостей
(по данным Positive Technologies на 2016 год)

Согласно данным Positive Technologies, наиболее часто уязвимости cookie встречаются на сайтах платежных систем и интернет-магазинов, что обусловлено пренебрежением средствами защиты [6]. Исключением являются лишь некоторые крупные игроки на рынке интернет-услуг, давно работающие в своей области и заботящиеся о своих клиентах [7].

Использование cookie в веб-браузерах значительно упрощает работу пользователей в Интернете. Есть много противоречивых мнений насчет того, важна ли конфиденциальность при использовании cookie. В целом вреда компьютеру нет, но в ряде случаев собранная информация может нанести вред самому пользователю, так как используются его личные данные [8]. И при всех этих удобствах использования не стоит забывать об обеспечении безопасности хранимых cookie.

Список литературы

1. Cookie [Электронный ресурс] // Wikipedia: Свободная энциклопедия. Режим доступа: https://ru.wikipedia.org/wiki/Cookie (дата обращения: 08.11.2017).

2. Простым языком об HTTP [Электронный ресурс] // Хабрахабр. Режим доступа: https://habrahabr.ru/post/215117/ (дата обращения: 08.11.2017).

3. Cookies [Электронный ресурс] // Cyberguru. Режим доступа: http://www.cyberguru.ru/dotnet/asp-net/cookies-beginners.html (дата обращения: 08.11.2017).

4. Cookie: что нужно знать? [Электронный ресурс] // Kaspersky lab Daily. Режим доступа: https://www.kaspersky.ru/blog/cookie-chto-nuzhno-znat/979/ (дата обращения: 08.11.2017).

5. Уязвимости веб-приложений: пора анализировать исходный код [Электронный ресурс] // Positive Research. Режим доступа: http://blog.ptsecurity.ru/2017/08/web-attacks.html (дата обращения: 08.11.2017).

6. *Хмельникова О. А.*, *Чудинова Е. В.* Обеспечение безопасности онлайн-покупок // Сб. тезисов докладов науч.-практ. конф. студентов Курган. гос. ун-та. Курган : Изд-во Курганского гос. ун-та, 2016. Вып. 17. С. 50.

7. *Скоробогатов Д. А.*, *Москвин В. В.* Безопасность электронных платежных систем на примере PayPal // Сб. материалов XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых «Безопасность информационного пространства». Курган, Курганский государственный университет, 2016. С. 202–205.

8. Не все cookie одинаково полезны [Электронный ресурс] // Хабрахабр. Режим доступа: https://habrahabr.ru/post/272187/ (дата обращения: 08.11.2017).

УДК 004.056.5

Е. Ю. Мищенко
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК СПОСОБ СНИЖЕНИЯ ЗАТРАТ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Обезличивание персональных данных как метод их защиты требует методологического обеспечения не только в плане подхода к реализации, но также в части обоснования эффективности как функциональной, так и экономической. В данной работе предлагается обоснование эффективности применения метода введения идентификаторов на основе критерия вероятности идентификации и рассматривается подход к реализации данного метода на базе запатентованной полезной модели. В результате внедрения метода в сфере здравоохранения был получен значительный экономический эффект.

Ключевые слова: персональные данные; обезличивание; метод идентификаторов.